



Policies and Procedures

Subject: Uses and Disclosures of Protected Health Information for Law Enforcement Purposes

Policy Number: HIPAA 4.5

Effective Date: 6/21/04

Entity Responsible: Division of General Counsel

Revision Date: 1/11/18

1. Purpose:

This policy provides instructions and guidelines for uses and disclosures of protected health information (PHI) for law enforcement purposes in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and under the Tennessee Code Annotated (T.C.A).

2. Policy:

- 2.1: The Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and the Regional Mental Health Institutes (RMHIs) shall disclose PHI or make PHI available for law enforcement purposes or elected officials, only as required by law.
- 2.2: The TDMHSAS or the RMHI must disclose PHI or make PHI available for use for law enforcement purposes under the following circumstances: (1) to a government authority or agency about an individual any employee reasonably believes is the victim of abuse, including sexual abuse, neglect, mistreatment, or believes is in imminent danger of harm. *See* TDMHSAS HIPAA Policy 4.4; (2) in the course of a judicial or administrative proceeding in response to a an order of a court or an administrative body, after the court determines that disclosure is necessary for the conduct of proceedings before it and that failure to make the disclosure would be contrary to public interest or the detriment of a party to the

proceedings. *See* TDMHSAS HIPAA Policy 4.1; or (3) to a law enforcement officials for certain law enforcement purposes pursuant to 45 C.F.R §164.512(f) when consistent with Tennessee law.

- 2.3: PHI must be disclosed without a court order, subject to certain limitations, to authorized federal officials for national security purposes, including intelligence, armed forces, public health, or protective services for the President of the United States, if the TDMHSAS Privacy Officer or the RMHI Privacy Officer reasonably believes PHI disclosure would prevent or lessen a serious of imminent threat of harm to a person or to the public.

3. Procedures:

- 3.1: The RMHI Privacy Officer must consult with the RMHI staff attorney concerning any request to disclose or use PHI received at the RMHI from law enforcement officials to determine whether PHI may be disclosed or made available for use. The TDMHSAS Privacy Office must consult with the TDMHSAS General Counsel concerning any request to disclose or use PHI from law enforcement officials to determine whether PHI may be disclosed or made available for use.
- 3.2: In instances concerning allegations of abuse, including sexual abuse, neglect, or mistreatment, any TDMHSAS or RMHI employee who receives a request for use or disclosure of PHI from the Department of Children's Services, the Department of Human Services, the TBI, the FBI, sheriff, law enforcement, or other official authorized to receive such information, must immediately, or as soon as practicable, refer the request to the TDMHSAS Central Privacy Officer or designee, or if the request occurs at an RMHI, to the RMHI Privacy Officer or designee, or RMHI staff attorney.
- 3.3: The RMHI must disclose allegations of felonious sexual offenses or bodily harm that appears to have been committed on RMHI premises to a law enforcement agency having jurisdiction. *See* TDMHSAS HIPAA Policy 4.1.
- 3.4: If the TDMHSAS Privacy Officer or the RMHI Privacy Officer or designee or RMHI staff attorney determines that PHI should be released to a law enforcement or other official, PHI must be released within ten (10) working days from the date of request. If PHI release is not appropriate, the TDMHSAS Privacy Officer or the RMHI Privacy Officer must notify the requesting party with ten (10) working days from the date of request.
- 3.5: The TDMHSAS or the RMHI Privacy officer/ designee who disclose PHI must document all disclosures, absent a valid authorization, on a disclosure log kept in the service recipient's record. A copy of the written request for disclosure must

also be placed in the service recipient's record. Disclosures of PHI may also be entered into an electronic log. This disclosure log should be kept for a minimum of six (6) years from the date the request for disclosure was received and this disclosure log shall be placed in the service recipient's file.

3.9.1: The disclosure log must include (1) date of the disclosure, (2) name of the individual of entity who received the PHI, and if known, their address, (3) a brief description of PHI disclosed, and (4) a brief statement of the purpose of the disclosure that reasonably describes the basis of the disclosure.

4. Other Considerations:

4.1: Authority:

45 CFR §164.512(a)(1), (f); TCA §§ 33-3-103, 108, 110, 111; 37-1-605; 71-6-103, 105.

Approved:

Marie Williams *vg*

Commissioner

1-11-18

Date